

**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings of claims in the application:

**Listing of Claims:**

- 1                    1. (Canceled) A token adapted to provide access to an account, the token  
2 comprising:  
  
3                    a memory configured to store an image of a biometric.
- 1                    2. (Canceled) The token of Claim 1 wherein said memory is an integrated circuit  
2 configured to store the image of the biometric.
- 1                    3. (Canceled) The token of Claim 2 wherein said biometric image is a finger  
2 print image stored in the memory in one of Tiff, JPEG and bitmap formats.
- 1                    4. (Canceled) The token of Claim 3 further comprising:  
  
2                    a magnetic stripe adapted to store data related to the account.
- 1                    5. (Canceled) The token of Claim 4 wherein said token is a card.
- 1                    6. (Canceled) The token of Claim 5 wherein said card is formed from material  
2 selected from a group consisting of plastic and metal.
- 1                    7. (Canceled) A system adapted to receive a token, said token comprising an  
2 integrated circuit memory configured to store an image of a biometric, said token adapted to  
3 provide access to an account, said system comprising:  
  
4                    a processor configured to read the biometric image stored in the integrated circuit  
5 memory disposed in the token.
- 1                    8. (Canceled) The system of Claim 7 wherein said processor is further  
2 configured to generate a binary number from the stored image of the biometric and in accordance  
3 with a preselected algorithm.

1                   9. (Presently amended) A system adapted to receive a token, said token  
2 comprising an integrated circuit memory configured to store an image of a biometric, said token  
3 adapted to provide access to an account, said system comprising:

4                   a processor configured to read the biometric image stored in the integrated circuit  
5 memory disposed in the token; wherein said processor is further configured to generate a binary  
6 number from the stored image of the biometric and in accordance with a preselected algorithm;  
7 and

8                   ~~The system of Claim 8 further comprising~~ a biometric sampler adapted to sample  
9 and capture an image of at least one biometric of the token holder at the location in which the  
10 system is stationed.

1                   10. (Original) The system of Claim 9 wherein said processor is further  
2 configured to generate a second binary number from the at least one biometric image of the  
3 token holder sampled and captured at the location in which the system is stationed, wherein said  
4 second binary number is generated in accordance with the preselected algorithm.

1                   11. (Original) The system of claim 10 wherein said processor is further  
2 configured to compare the first and second binary numbers to determine whether they match  
3 within a predefined tolerance limit.

1                   12. (Original) The system of 11 wherein said processor is further configured to  
2 generate a third binary number from one of the first and second binary numbers if the first and  
3 second binary numbers match each other within the predefined tolerance limit, wherein said third  
4 binary number is generated in accordance with a second preselected algorithm.

1                   13. (Original) The system of claim 12 wherein said third binary number has  
2 fewer bits than either of the first and second binary numbers.

1                   14. (Original) The system of Claim 13 further comprising a second processor  
2 configured to receive the third binary number from the first processor.

1                   15. (Original) The system of Claim 14 wherein said first and second processors  
2 are located at different sites.

1                   16. (Original) The system of Claim 15 wherein said second processor receives  
2 the third binary number from the first processor via wired or wireless communication lines.

1                   17. (Original) The system of Claim 16 wherein said second processor is coupled  
2 to a database which maintains a fourth binary number extracted from a same biometric image  
3 source from which the biometric image stored in the memory is supplied, wherein said fourth  
4 binary number is extracted in accordance with the second preselected algorithm.

1                   18. (Original) The system of Claim 17 wherein said second processor is  
2 configured to retrieve the fourth binary number from the database and compare the retrieved  
3 fourth binary number to the third binary number it receives from the first processor to determine  
4 whether a match exists between the third and fourth binary numbers within a second predefined  
5 tolerance limit.

1                   19. (Original) The system of Claim 18 wherein if the second processor  
2 determines that a match exists between the third and fourth binary numbers then access to the  
3 account associated with the token is granted.

1                   20. (Original) The system of Claim 19 wherein if the first processor determines  
2 that the first and second binary numbers do not match each other within the first predefined  
3 tolerance limit then access to the account associated with the token is denied.

1                   21. (Original) The system of Claim 20 wherein if the second processor  
2 determines that the third and fourth binary numbers do not match each other within a second  
3 predefined tolerance limit then access to the account associated with the token is denied.

1                   22. (Original) The system of Claim 21 wherein the second processor further  
2 receives information related to the account with which the token is associated with from the first  
3 processor.

1                   23. (Original) The system of Claim 22 further comprising:  
  
2                               a key pad configured to enable the token holder to enter information  
3 related to the account into the system; and  
  
4                               a display configured to display messages to the token holder.

1                   24. (Original) The system of Claim 23 further comprising:  
  
2                               a magnetic read device adapted to receive information stored on a magnetic  
3 medium disposed on the token.

1                   25. (Original) The system of Claim 24 wherein the at least one biometric sample  
2 is a finger print sample and wherein the image of the at least one biometric sample of the token  
3 holder sampled and captured by the biometric sampler is formatted according to one of Tiff,  
4 bitmap and JPEG image format standards.

1                   26. (Canceled) A method of forming a token adapted to provide access to an  
2 account, the method comprising:

3                               forming a memory;

4                               storing an image of a biometric in the memory; and

5                               disposing the memory on the token.

1                   27. (Canceled) The method of Claim 26 wherein said memory is an integrated  
2 circuit memory configured to store the image of the biometric.

1                   28. (Canceled) The method of Claim 27 wherein said biometric image is a finger  
2 print image.

1                   29. (Canceled) The method of Claim 28 wherein said finger print image is stored  
2 in the memory in one of Tiff, bitmap and JPEG formats.

1                   30. (Canceled) The method of Claim 29 further comprising:  
2 disposing a magnetic stripe adapted to store data related to the account on the  
3 token.

1                   31. (Canceled) The method of Claim 30 wherein said token is a card.

1                   32. (Canceled) The method of Claim 31 wherein said card is formed from  
2 material selected from a group consisting of plastic and metal.

1                   33. (Cancel) A method of authorizing access to an account with a token, the  
2 method comprising:

3                   receiving the token on which a memory configured to store an image of a  
4 biometric is disposed; and

5                   reading the biometric image stored in the memory disposed on the token.

1                   34. (Presently amended) A method of authorizing access to an account with a  
2 token, the method comprising:

3                   receiving the token on which a memory configured to store an image of a  
4 biometric is disposed;

5                   reading the biometric image stored in the memory disposed on the token; and ~~The~~  
6 ~~method of Claim 33 further comprising:~~

7                   generating a binary number from the biometric image stored in the memory in  
8 accordance with a preselected algorithm.

1                   35. (Original) The method of Claim 34 further comprising:  
2                   capturing at least one biometric image of the token holder at the location in which  
3                   access to the account associated with the token is requested.

1                   36. (Original) The method of claim 35 further comprising:  
2                   generating a second binary number from the at least one biometric image captured  
3                   from the token holder in accordance with the preselected algorithm.

1                   37. (Original) The method of claim 36 further comprising:  
2                   comparing the first and second binary numbers to determine whether they match  
3                   within a predefined tolerance limit.

1                   38. (Original) The method of claim 36 further comprising:  
2                   extracting a third binary number from one of the first and second binary numbers  
3                   if the first and second binary numbers match each other within the predefined tolerance limit,  
4                   wherein said third binary number is extracted in accordance with a second preselected algorithm.

1                   39. (Original) The method of Claim 38 wherein said third binary number has  
2                   fewer bits than the first and second binary numbers.

1                   40. (Original) The method of Claim 39 further comprising transmitting the third  
2                   binary number to another location via wired or wireless communication lines.

1                   41. (Original) The method of Claim 40 further comprising:  
2                   comparing the transmitted third binary number to a fourth binary number  
3                   maintained in a database to determine whether a match exists between the third and fourth binary  
4                   numbers within a second predefined tolerance limit, wherein said fourth binary number is  
5                   extracted from a same biometric image source from which the biometric image stored in the

6 memory is supplied, wherein said fourth binary number is extracted in accordance with the  
7 second preselected algorithm; and

8 granting access to the account associated with the token if the third and fourth  
9 binary numbers match within a second predefined tolerance limit.

1 42. (Original) The method of Claim 41 further comprising:  
2 denying access to the account associated with the token if the third and fourth  
3 binary numbers do not match within the second predefined tolerance limit.

1 43. (Original) The method of Claim 42 further comprising:  
2 transmitting account related information via the wired or the wireless  
3 communication lines, wherein the account related information are retrieved from the token.

1 44. (Original) The method of Claim 43 further comprising:  
2 receiving information related to the account from the token holder; and  
3 displaying messages related to the account to the token holder.

1 45. (Original) The method of Claim 43 further comprising:  
2 storing account related information on a magnetic stripe disposed on the  
3 token.

1 46. (Original) The method of Claim 45 wherein biometric image is stored in the  
2 memory according to one of Tiff, bitmap and JPEG image format standards.

1 47. (Original) The method of Claim 46 wherein said biometric is a finger print.

1 48. (Original) The method of Claim 47 wherein said memory is an integrated  
2 circuit memory.